37597pr2-am P-044 7MAR01

#9/B

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In Re Application of : Kipnis et al.
Serial No. : 09/552,115
Filed : April 19, 2000
For : PUBLIC-KEY SIGNATURE METHODS AND SYSTEMS

Group Art Unit: **Not Yet Assigned**
Examiner: **Not Yet Assigned**

Hon. Commissioner of Patents and Trademarks
Washington, D.C. 20231

Sir:

PRELIMINARY AMENDMENT

In order to place the application in better condition for examination, kindly amend the above identified application as follows:

In the specification:

Page 2, kindly add after the words "September 1997." that end the second full paragraph:

B1

--In the basic form of the "Oil and Vinegar" scheme computation of a signature x of y is performed as follows:

Step 1: $y = (y_1,\ldots,y_n)$ is transformed into b = $(b_1,\ldots,b_n)$ such that $b = t^{-1}(y)$, where t is the secret, bijective, and affine function from K^n to K^n.

Step 2: We find n variables $a_1,\ldots,a_n$ of K, and n variables $a'_1,\ldots,a'_n$ of K, such that the n equations (S) are satisfied:

$$\forall i,\ 1 \le i \le n, \quad b_i = \Sigma\gamma_{ijk}a_j a'_k + \Sigma\lambda_{ijk}a'_j a'_k + \Sigma\xi_{ij}a_j + \Sigma\xi'_{ij}a'_j + \delta_i. \quad (S)$$

This can be done as follows: we choose at random the n variables a'_i, and then we compute the a_i variables from (S) by Gaussian reductions (because - since there are